WHAT IS CLAIMED IS:

1. A method for achieving data encryption and/or key expansion/generation, said method comprising the steps of:

providing a short, shared, secret, seed key between first and second parties, the seed key allowing the first and second parties to encrypt and decrypt messages transmitted between the first and second parties;

extending the seed key to a long extended key;

using the running keys to choose one of many possible quantum or classical signal sets embodied in a number of modes of electromagnetic or acoustic or other physical origins; and

adjusting the signal strength of each signal in the signal sets in accordance with the number of signal sets to obtain a desired security level, wherein quantum or classical noise in the system hides both encrypted data bits and the running key prevents a third evesdropping party from success in compromising message transmissions between the first and second parties.

2. The method according to claim 1, wherein the signal sets are based on a number of modes of energy carrying waves either in free space or in guided media.

3. The method according to claim 2, wherein the energy bearing waves are electromagnetic waves, including radio waves, microwaves, millimeter waves, or light waves.

4. The method according to claim 2, wherein the modes are two modes of the light waves, and wherein the two modes of light waves are polarization modes, time or frequency modes, spatial modes or any combination of such physical attributes of the light waves.

5. The method according to claim 1, implemented over all types of networks, including enterprise, metro, short haul, and long haul, and independent of underlying software protocols.

6. A method for encrypting data, said method comprising the steps of:

generating a large number of quantum signal sets of low to high energy; and

modulating the sets of quantum signal with the data being encrypted by using a multi-bit seed key suitably extended to obtain running keys to select quantum signal sets for different bit values, whereby each quantum signal set is encoded into a coherent state of an infinite-dimensional space or any other quantum state in space of any dimension.

7. The method according to claim 6, including the step of extending the multi-bit seed key K into a

much longer extended key K' and using the extended key K' to determine for each qumode carrying bit, b (0,1), which quantum signal set is to be used.

8. The method according to claim 7, wherein the extended key K' includes 2^s-1 bits, where s is the number of bits of the seed key K, and wherein using the extended key K' to determine qumodes includes segmenting the extended key K' into disjointed blocks of r-bit running keys R, where $r = \log_2(M)$ and $s >> r$, wherein r is the number of bits of each of the running keys R, and M is the number of bases for the coherent states.

9. The method according to claim 6, wherein each quantum signal set is composed of any number of photons from small to large, and including the step of coding all of the photons of a given quantum signal set to represent a bit value for that quantum signal set.

10. The method according to claim 6, wherein each quantum signal set defines a bit value, and wherein the number of bases M for the coherent states is much larger than the average number of photons $|\alpha_0|$ used to encode a given bit value.

11. A method for encrypting data, said method comprising the steps of:

providing a multi-bit seed key;

extending the multi-bit seed key K to produce a multi-bit extended key K', the length of the extended key being substantially greater than the length of the seed key K;

segmenting the extended key K' into a plurality of disjointed running keys R; and

modulating an energy bearing wave using the running keys R to select different bit values for different portions of the energy bearing wave to thereby encrypt the energy bearing wave with the data.

12. The method according to claim 11, wherein the energy bearing wave is an electromagnetic wave, including a radio wave, a microwave, a millimeter waves, or a light wave.

13. The method according to claim 11, wherein the extended key K' includes 2^s-1 bits, where s is the number of bits of the seed key K.

14. The method according to claim 13, wherein the step of segmenting the extended key K' into blocks includes segmenting the extended key K into blocks of r-bit running keys R, where r is the number of bits of each of the running keys R, and $s >> r$.

15. A method for encrypting data, said method comprising the steps of:

producing a light signal that includes a plurality of polarization-mode coherent states of light;

extending a multi-bit seed key K to produce a multi-bit extended key K' the length of which is substantially greater than the length of the seed key K;

segmenting the extended key K' into a plurality of disjointed blocks of running keys R, each being r bits in length; and

modulating a finite number of the polarization-mode states of light using the running keys R to produce a multi-bit information bearing light signal.

16. The method according to claim 15, wherein the polarization-mode states comprise two-mode coherent states of light, and including the step of using the extended key K' to determine, for each qumode carrying bit, b (0,1), which pair of signals is to be used.

17. The method according to claim 15, wherein each quantum signal set includes at least about 1,000 photons, and including the step of coding all of the photons of a given quantum signal set to represent a bit value for that quantum signal set.

18. The method according to claim 17, and including the step of coding all of the photons of a given quantum signal set to represent a bit value

for that quantum signal set, wherein the number of bases M for the coherent states is much larger than the average number of photons $|\alpha_0|$ used to encode a given bit value.

19. The method according to claim 15, wherein the extended key K' includes 2^s-1 bits, where s is the number of bits of the seed key K.

20. The method according to claim 15, wherein signal components of the light signal are macroscopically distinguishable.

21. The method according to claim 15, wherein the extended key K' is segmented into disjointed blocks of r-bit running keys R, where $r = \log_2(M)$ and $s >> r$, r is the number of bits of each of the running keys R, and M is the number of bases.

22. A method for encrypting data, said method comprising the steps of:

producing a light signal that includes two-mode coherent states of light;

extending a multi-bit seed key K to produce a multi-bit extended key K', the length of which is substantially greater than the length of the seed key K;

segmenting the extended key K' into a plurality of disjointed blocks of running keys R, each of the running keys being r-bits in length; and

modulating a finite number of the two-mode coherent states of light using the running keys R to produce a multi-bit information bearing light signal.

23. The method according to claim 22, wherein producing the light signal includes projecting light from a source of light equally into first and second polarization modes of light.

24. The method according to claim 23, wherein modulating the two-mode coherent states of light includes introducing a relative phase shift between the first and second polarization modes of light.

25. The method according to claim 23, wherein the relative phase shift introduced between the first and second polarization modes of light is in the range of about 0-2π radians.

26. The method according to claim 22, wherein the number of bases M for the coherent states of light is much larger than the number of photons $|\alpha_0|$ used to encode a given bit value.

27. The method according to claim 22, wherein signal components of the light signal are macroscopically distinguishable.

28. The method according to claim 23, wherein the extended key K' includes 2^s-1 bits, where s is the number of bits of the seed key K.

29. The method according to claim 28, wherein the number of bits r of each block is equal to $\log_2(M)$ and s >> r, where M is the number of bases formed by the first and second polarization states of light and s is the number of bits of the seed key K.

30. A method for transmitting data between first and second locations, said method comprising the steps of:

encrypting data to be transmitted by

producing at the first location a plurality of polarization-mode coherent states of light at a first location;

extending a multi-bit seed key K to produce a multi-bit extended key K', the length of which is substantially greater than the length of the seed key K;

segmenting the extended key K' into a plurality of disjointed blocks of running keys R, each of the running keys being r-bits in length; and

modulating a finite number of the polarization-mode coherent states of light using the running keys to produce a multi-bit information bearing light signal;

transmitting the information bearing light signal over a communication channel from the first location to the second location; and

decrypting the transmitted data at the second location including

extending the same multi-bit seed key K at the second location to produce the extended key K', the length of which is substantially greater than the length of the seed key K;

segmenting the extended key K' into a plurality of disjointed blocks of running keys R, each of the running keys being r-bits in length;

applying unitary transformations to the received polarization states according to the extended key K', wherein the relative phase shift introduced is determined by the extended key K' generated and applied to the information bearing light signal; and

processing the received information bearing light signal to cancel polarization rotation caused by communication channel, whereby after the phase shift has been applied, the relative phase shift between the first and second polarization modes is 0 or π radians corresponding to logic 1 and logic 0 bits, respectively, according to the extended key K'.

31. The method according to claim 30, wherein each quantum signal set includes at least about 1,000

photons, the photons of a given quantum signal set coded to represent a bit value for that quantum signal set. and wherein the number of bases M for the coherent states is much larger than the number of photons $|\alpha_0|$ used to encode a given bit value.

32. The method according to claim 30, wherein each quantum signal set defines a bit value, and wherein the number of bases M for the coherent states is much larger than the average number of photons $|\alpha_0|$ used to encode a given bit value.

33. The method according to claim 30, wherein each bit of the information bearing light signal is defined by a number of photons in the range of about 1,000 to about 100,000 photons.

34. The method according to claim 30, including amplifying the information bearing light signal as prior to processing the information bearing light signal at the second location.

35. The method according to claim 30, wherein extending the seed key includes using the seed key K to drive an encryption mechanism to produce the extended key K'.

36. A method for transmitting data, said method comprising the steps of:

encrypting at a first location data to be transmitted by

producing a light signal that includes two-mode coherent states of light;

extending a multi-bit seed key K to produce a multi-bit extended key K', the length of which is substantially greater than the length of the seed key K;

segmenting the extended key K' into a plurality of disjointed blocks of running keys R, each of the running keys being r-bits in length; and

modulating a finite number of the two-mode states of light using the running keys to produce a multi-bit information bearing light signal;

transmitting the information bearing light signal, including the modulated polarization states of light from the first location to a second location through a communication channel; and

decrypting the transmitted data at the second location including

extending the same seed multi-bit K to produce the extended key K', the length of which is substantially greater than the length of the seed key K;

applying unitary transformations to the received polarization states according to the extended key by using a modulator to introduce relative phase shift determined by the extended key K' generated and applied to the information bearing light signal; and

processing the information bearing light signal to cancel the polarization rotation caused by the communication channel, whereby after the phase shift has been applied, the relative phase shift between the polarization modes is 0 or π corresponding to logic 1 or logic 0 according to the extended key.

37. The method according to claim 36, wherein the communication channel is a guided media.

38. The method according to claim 36, wherein producing the light signal includes projecting light from a source of light equally into two polarization modes of light.

39. The method according to claim 36, wherein modulating the two-modes states of light at the first location includes introducing a relative phase shift between the two polarization modes of light.

40. The method according to claim 39, wherein the relative phase shift introduced between the two polarization modes of light is in the range of about $0-2\pi$ radians.

41. The method according to claim 40, wherein the number of bases M for the coherent states is much larger than the average number of photons $|\alpha_0|$ used to encode a given bit value.

42. The method according to claim 40, including amplifying the information bearing light signal while the information bearing light signal is being transmitted from the first location to the second location.

43. The method according to claim 40, wherein a seed key K drives an encryption mechanism the output of which is a much longer extended key K' that is used to determine which pair of signals is to be used for each qumode carrying bit b (0,1).

44. The method according to claim 40, and including using a seed key extended to a longer key to modulate the parameters of a multi-mode coherent states of light.

45. The method according to claim 44, and including using an encryption mechanism to extend the short seed key K.

46. The method according to claim 40, wherein processing the light signal includes future rotating the received polarization states of light by an amount equal to $\pi/4$.

47. The method according to claim 40, wherein signals of each pair of light signals are macroscopically distinguishable.

48. A communication system comprising:

means for generating a large number of quantum signal sets of low to high energy; and

means for modulating the sets of quantum signal with the data being encrypted by using a multi-bit seed key to select quantum signal sets for different bit values, whereby each quantum signal set is encoded into a coherent state of an infinite-dimensional space.

49. The system according to claim 48, including means for extending the multi-bit seed key K into a much longer extended key K' that is used to determine for each qumode carrying bit b (0,1), which quantum signal set is to be used.

50. The system according to claim 49, wherein the extended key K' includes 2^s-1 bits, where s is the number of bits of the seed key K.